UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

AMELIA INGRAO and ELISABETH PACANA, individually and on behalf of all others similarly situated, Plaintiff, v. ADDSHOPPERS, INC., NUTRISYSTEM, INC., VIVINT, INC., Defendants.	Case No. 2:24-cv-1022

PLAINTIFFS' SUPPLEMENTAL BRIEFING

Plaintiffs allege a traditional wiretapping scheme by AddShoppers and the retail defendants using modern technology. The retail defendants install AddShoppers' SafeOpt tracking code on their website. Compl. ¶ 36. This tracking code functions like a wiretap device, transmitting the consumer's activities on the retailer's website to AddShoppers. *Id*. ¶ 37. AddShoppers then compiles this data with a consumer's personal information to create detailed user profiles, *id*. ¶ 3, 29, 32, 39, which are later used to send targeted advertisements, *id*. ¶ 32, 41. The only court to confront this mass surveillance scheme held Plaintiffs adequately alleged both standing and a substantive violation of California's wiretapping law.

None of Defendants' six arguments at the hearing suggest these claims should be treated differently here. *See* September 23, 2024 Motions Hearing Transcript (Tr.). First, the Court can exercise personal jurisdiction over AddShoppers under the traditional jurisdictional test. Second, Plaintiffs suffered a concrete injury when AddShoppers tracked their online activity aided by Nutrisystem and Vivint. Third, AddShoppers is not a direct party to Plaintiff Ingrao's communication with Nutrisystem's website and thus is a third-party wiretapper. Fourth,

AddShoppers collected the substantive content of Plaintiffs' communications with retailers. Fifth, Plaintiffs did not consent to AddShoppers' wiretaps simply by accessing Vivint's website. And finally, it is premature to determine where Plaintiff Ingrao's communications were intercepted. These arguments are taken in turn.

A. The Court can exercise specific jurisdiction over AddShoppers under the traditional test.[1]

The Court can comfortably exercise specific jurisdiction over AddShoppers under the traditional test. *See Hasson v. FullStory, Inc.*, 114 F.4th 181, 197 (3d Cir. 2024) (remanding for the district court to consider whether it could exercise personal jurisdiction over a software tracking company under the traditional test). Specific jurisdiction exists when: (1) the defendant purposefully directs conduct at the forum state, creating contacts with forum; (2) the plaintiff's claims arise out of or relate to those contacts; and (3) the exercise of jurisdiction satisfies notions of fair play and substantial justice. *Havassy v. Keller Williams Realty, Inc.*, 2024 WL 1640984, at *4 (E.D. Pa. Apr. 16, 2024); *see also* Tr. at *11 (outlining traditional personal jurisdiction test). Each requirement is met here.

1. AddShoppers purposefully directed conduct toward Pennsylvania.

AddShoppers "purposely availed itself of the privilege of doing business in Pennsylvania through its activities here." *Havassy.*, 2024 WL 1640984, at *4. It entered into agreements with numerous Pennsylvania companies, including Nutrisystem, to install its code on their websites. Compl. ¶ 14; *Havassy*, 2024 WL 1640984, at *4 (agreements in the state supported purposeful availment). And "it sends thousands (if not millions) of targeted emails to Pennsylvania" to exploit the Commonwealth's retail market. Compl. ¶ 14; Tr. at *13 (AddShoppers' counsel

[1] Neither Nutrisystem nor Vivint seeks dismissal for lack of personal jurisdiction. Tr. at *21-22.

acknowledging it must do some advertising to potential retail partners); *Havassy*, 2024 WL 1640984, at *4 (advertising in the state supported purposeful availment). It then derives revenue from every purchase made based on those emails. Compl. ¶ 3. "Unquestionably, [AddShoppers] has created contacts with Pennsylvania from which it benefits, satisfying the purposeful direction requirement." *Havassy*, 2024 WL 1640984, at *4.

2. Plaintiffs' claims relate to AddShoppers' contacts with Pennsylvania.

Plaintiffs' wiretapping claims share a strong relationship to AddShoppers' forum related contacts. *See Havassy*, 2024 WL 1640984, at *5–6 (plaintiff's claims arose out of forum related contacts where the agreements led to the offending telephone calls); *see also Gentex Corp. v. Abbott*, 978 F. Supp. 2d 391, 400 (M.D. Pa. 2013) ("[I]t is apparent that but for Defendant Abbott's Pennsylvania-related phone conversations and internet activity, the shipment of allegedly infringing products to Pennsylvania and these subsequent claims would not have occurred in this jurisdiction."). AddShoppers' agreements with Pennsylvania retailers are for the "express purpose of enabling AddShoppers to collect customer data and conduct unsolicited customer outreach." *McClung v. AddShopper, Inc.*, 2024 WL 189006, at *1 (N.D. Cal. Jan. 17, 2024). And because AddShoppers' email advertisements depend on its illegal tracking, the thousands or millions of target emails to Pennsylvanians are also closely tied to Plaintiffs' wiretapping claims. Simply put, Plaintiffs' claims arise out AddShoppers' conduct in Pennsylvania.

3. The Court exercising personal jurisdiction reflects fair play and substantial justice.

AddShoppers cannot show personal jurisdiction is inconsistent with fair play and substantial justice. "When determining reasonableness, courts consider 'the burden on the defendant, the forum State's interest in adjudicating the dispute, the plaintiff's interest in obtaining convenient and effective relief, the interstate judicial system's interest in obtaining the most

efficient resolution of controversies, and the shared interest of the several States in furthering fundamental substantive social policies.'" *Elan Chem. Co. v. Adams Extract & Spice LLC*, 2024 WL 3755823, at *3 (D.N.J. Aug. 12, 2024). Here, Pennsylvania passed one of the most protective wiretap statutes in the United States because it has a strong interest in protecting its citizens against the privacy violations inherent in unconsented, undisclosed interceptions of their personal information. *See Dance v. Com., Pennsylvania State Police*, 726 A.2d 4, 8 (Pa. Commw. Ct. 1999) ("The focus and purpose of the Wiretap Act is protection of privacy. . . . As such, the provisions of the Wiretap Act must be strictly construed."). Nor can AddShoppers make a "compelling case that litigation in Pennsylvania would be unreasonable and unfair." *Gentex Corp. v. Abbott*, 978 F. Supp. 2d 391, 401 (M.D. Pa. 2013) (quotations and citations omitted). AddShoppers had no issue partnering with Pennsylvania companies or targeting its residents when it financially benefited from the relationship, so it is entirely fair and reasonable to hold AddShoppers accountable in the Commonwealth whose laws it violated. At most, AddShoppers can argue that it must travel to this forum, but courts have repeatedly rejected arguments this burden is unreasonable. *Id*. "When minimum contacts have been established, often the interests of the plaintiff and the forum in exercise of jurisdiction will justify even the serious burdens placed on the alien defendant." *Asahi Metal Indus. Co. v. Superior Court*, 480 U.S. 102, 114 (1987).

B. Plaintiffs have a concrete privacy injury sufficient to create Article III standing.[2]

Defendants' wiretapping scheme caused Plaintiffs to suffer concrete and particularized injuries to their privacy interests. By aggregating Plaintiffs' browsing activities with their personal

[2] At times, Vivint has suggested the Court should dismiss the case for lack of standing with prejudice. But the Court can only dismiss a case for lack of standing *without* prejudice. *See Barclift v. Keystone Credit Serv., LLC*, 93 F.4th 136, 140 (3d Cir. 2024) ("We agree that Barclift lacks standing, but we will modify the District Court's order so that the dismissal will be without prejudice.").

information, AddShoppers creates detailed user profiles without their knowledge or consent.[3] This constitutes an injury-in-fact under Supreme Court and this Circuit's precedent.

In *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), the U.S. Supreme Court addressed the question: "[w]hat makes a harm concrete for purposes of Article III?" *Id*. at 424. The Court explained that "history and tradition offer a meaningful guide to the types of cases that Article III empowers federal courts to consider." *Id*. (quotations omitted). Specifically, the Court instructed that courts should look at whether the plaintiff's injury "has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id*. The Court noted concrete harm is not limited to "physical harms and monetary harms" but that "[v]arious intangible harms can also be concrete." *Id*. at 425. The Court gave examples of intangible harms recognized at common law, including "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id*. (collecting cases).

TransUnion aligns with prior holdings from the Third Circuit. Indeed, the Third Circuit has long recognized that "unauthorized disclosures of information have long been seen as injurious" and that "improper dissemination of information can itself constitute a cognizable injury." *In re Horizon Healthcare Servs. Inc. Data Breach Litig*., 846 F.3d 625, 638-39 (3d Cir. 2017) (cleaned up). In *In re Nickelodeon Consumer Privacy Litig*., 827 F.3d 262 (3d Cir. 2016),

---

[3] During the hearing, the parties discussed the types of personal information associated with AddShoppers' detailed user profiles. Plaintiffs focused on one form of personal information, email addresses. Tr. at *35-36; *see Atl. Coast Life Ins. Co. v. A.M. Best Rating Servs., Inc.*, 2024 WL 3582248, at *1 (D.N.J. June 25, 2024) ("The District of New Jersey has similarly recognized that personally identifying information is properly sealed, including e-mail addresses and other personal information where inclusion of that information is unnecessary."); CA Civ. Code § 1798.140(o)(1) (defining personal information to include, among other things, "unique personal identifier, online identifier, internet protocol address, email address . . . or other similar identifier."). The AddShoppers profile may also include other personal information like IP addresses, phone numbers, browser characteristics, cookies, and session information.

for example, the Third Circuit considered whether a concrete injury existed when a website operator informed users that it would not track the browsing and video-watching habits of children but then compiled their web activity with their account information to sell targeted advertising. *Id*. at 269. In finding an injury-in-fact, the Third Circuit held that "[t]he purported injury here is clearly particularized, as each plaintiff complains about the disclosure of information relating to his or her online behavior. While perhaps 'intangible,' the harm is also concrete in the sense that it involves a clear *de facto injury, i.e*., the unlawful disclosure of legally protected information." *Id*. at 274.

In *In re: Google Inc. Cookie Placement Consumer Priv. Litig*., 934 F.3d 316 (3d Cir. 2019), the Third Circuit considered similar harms where web users alleged that internet advertising providers collected private data regarding their personal internet browsing by circumventing their cookie blockers. *Id*. at 325. As in *Nickelodeon*, the Court held that the surreptitious collection of information gave rise to an injury-in-fact for purposes of Article III standing, noting:

> More than precedent supports our conclusion. History and tradition reinforce that a concrete injury for Article III standing purposes occurs when Google, or any other third party, tracks a person's internet browser activity without authorization. Privacy torts have become "well-ensconced in the fabric of American law." *In re Horizon Healthcare Servs. Inc. Data Breach Litig*., 846 F.3d 625, 638 (3d Cir. 2017). Indeed, as Justice Thomas has explained, private actions to remedy intrusions on the private sphere trace back to England, where a property owner needed only to show that another person placed a foot on his property to establish a traditional case or controversy. *See Spokeo*, 136 S. Ct. at 1551 (Thomas, J., concurring) (citing *Entick v. Carrington*, 2 Wils. K.B. 275, 291 (1765)). Likewise, "Congress has long provided plaintiffs with the right to seek redress for unauthorized disclosures of information that, in Congress's judgment, ought to remain private." *Nickelodeon*, 827 F.3d at 274. In an era when millions of Americans conduct their affairs increasingly through electronic devices, the assertion Google makes—that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data—is untenable. Nothing in *Spokeo* or any other Supreme Court decision suggests otherwise.

Id.

Earlier this year, the Western District of Pennsylvania considered whether a website user experienced a concrete injury where he alleged violations of the Pennsylvania Wiretap Act after

he was browsing a website and "Facebook's Tracking Pixel" captured his activity on the website and sent it back to Facebook without his consent. *See Petris v. Sportsman's Warehouse, Inc*., 2024 WL 2817530, at *1 (W.D. Pa. June 3, 2024). The *Petris* Court examined the relevant cases and noted that "[t]he litigants of all three cases—*TransUnion, Google, Nickelodeon*—were all found to have standing after they were allegedly personally harmed, whether it be the furtive capture or surreptitious disclosure of their personal information. While *TransUnion* can be differentiated from *Nickelodeon* or *Google* by the nature of the harm at issue, all three cases deal with traditionally recognized harms." *Id*. at *5. The Court held that the plaintiff had standing for at least two reasons: (1) "because at least some of the information [the plaintiff] alleged was intercepted and shared with third parties amounts to a clear de facto injury. A 'de facto injury, *i.e*., the unlawful disclosure of legally protected information,' is enough to confer standing; and (2) the plaintiff's alleged harms are "analogous to the right to privacy in communications embodied in the common law and [the Pennsylvania Wiretap Act]" because "[t]he common law right to privacy has its roots in the long-established recognition that citizens have a protectable interest in their private information and in the sanctity of their communications that may not be disseminated to third parties without their knowledge and consent." *Id*. at *6 (noting that "[b]oth the common law right to privacy and a cause of action under [the Pennsylvania Wiretap Act] address the same interest: a person's control of private information concerning his or her private information.").

For the same reasons held in *TransUnion*, *Nickelodeon*, *Google*, and *Petris*, the harms alleged here bear a close relationship to those recognized at common law, including public disclosure of private information and the common law right to privacy regarding personal

information.[4] *See Braun v. Philadelphia Inquirer, LLC*, 2023 WL 7544160, at *5 (E.D. Pa. Nov. 13, 2023) (denying motion to dismiss for lack of standing where plaintiffs alleged Philadelphia Inquirer transmitted to Facebook information that allowed Facebook to identify which videos each plaintiff had viewed on the website); *James v. Walt Disney Co.*, 701 F. Supp. 3d 942, 947–52 (N.D. Cal. 2023) (standing to pursue wiretapping claims against website operator where the software captured and collected the precise web pages viewed by the plaintiffs); *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 942–43 (N.D. Cal. 2022) (standing to pursue wiretapping claims where defendant secretly observed, collected, and analyzed real-time information about everyone using its platform and services). And because the wiretapping scheme relies on the participation of retailers like Nutrisystem and Vivint, California and Pennsylvania law treats them as principals to the act. Their knowing participation as wiretappers "is enough to confer standing for a victim of the scheme to sue that retailer in federal court." *McClung*, 2024 WL 189006, at *2.

Yet Defendants seek to downplay the privacy harm by misrepresenting how the tracking scheme operates and the information it captures. For example, Vivint argues Plaintiffs lack standing because they did not provide personal information to the website. Tr. at *23, *27-28, *61. But as *McClung* explains, "[t]he whole idea of AddShoppers' scheme is to tie browsing activity on one site with personal information disclosed on another site, obviating the need for the retailers to do it themselves." *McClung*, 2024 WL 189006, at *2 n.1 (emphasis in original). That is, the

[4] Courts and third parties alike have recognized that the aggregation of a person's detailed browsing history with their personal information constitutes a privacy injury. *See McClung*, 2024 WL 189006, at *2; *see also* Federal Trade Commission, *A look behind the screens: Examining the data practices of social media and video streaming services* [Staff Report], at *40, (accessed at https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf) (recognizing the many harms from aggregation); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 505-09 (2006) (recognizing the privacy injury from aggregating data).

tracking code allows AddShoppers to associate a consumer's detailed browsing activity with their personal information, creating a privacy violation precisely *because* they do not directly provide any personal information to the website.

Defendants also repeatedly argue Plaintiffs only allege the tracking code generally captured the website visited and the time it was visited. Tr. at *18, *20. This is incorrect. Plaintiffs assert that AddShoppers' tracking code automatically collects detailed browsing data, including the exact webpages viewed. *See* Section C.2. Similarly, Vivint's focus on whether Plaintiff Pacana received an email misses the point. Tr. at *31. Users who are unwittingly placed in the AddShoppers network may or may not receive a targeted advertising email, but the injury occurs when their browsing data is captured without consent. An email simply confirms that tracking occurred, while the actual harm arises from the unauthorized collection of private browsing activity.

As here, the Third Circuit has consistently held plaintiffs suffer a concrete injury when their personal browsing history is secretly collected, compiled into a personal profile, and used for advertising. *See, e.g., In re Nickelodeon*, 827 F.3d 262 (concrete injury where website operator deceptively compiled web activity with account information to sell advertising); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316 (concrete injury where internet search engine secretly compiled web browsing history to serve targeted advertisements). Indeed, Plaintiffs' "common law right to privacy has its roots in the long-established recognition that citizens have a protectable interest in their private information and in the sanctity of their communications that may not be disseminated to third parties without their knowledge and consent." *Petris*, 2024 WL 2817530, at *6 ; Tr. at *26 (Vivint arguing the concrete harm must be consistent with a traditional claim); Tr. at *52 (same). Although "the right to privacy as to wiretapping" was "originally ingrained into the common law," the right is now largely enshrined

by federal and state statutes like CIPA and the Pennsylvania Wiretap Act. *Petris*, 2024 WL 2817530, at *6 (cleaned up). "Like the common law, [those statutes] protects the privacy rights of individuals. Specifically, [the statutes] guards these privacy rights by regulating interception and disclosure of wire, electronic, and oral communications." *Id*. (citations omitted).

Vivint's cases do not implicate the same privacy harm.[5] To the contrary, they involve a different type of software (session replay) which collects anonymized data from a single website to improve the website's performance for visitors. *See Cook v. GameStop, Inc.*, 689 F.Supp.3d 58, 66 (W.D. Pa. 2023) ("That Ms. Cook's browsing activity here was anonymous is particularly significant and dooms any attempt to establish a concrete injury in fact."); *Massie v. General Motors LLC*, 2022 WL 534468, at *5 ("Plaintiffs fail to explain how either GM's or Decibel's possession of anonymized, non-personal data regarding their browsing activities on GM's website

[5] Vivint has only offered one case analyzing standing for claims related to a similar tracking technology: *In re BPS Direct, LLC*, 705 F.Supp.3d 333, 362-365 (E.D. Pa. 2023). But because it misapplies the Supreme Courts test from *TransUnion*, it is contrary the great weight of authority. The Supreme Court is clear: Plaintiffs need not provide an "exact duplicate" between the common law harm and the statutory violation. *Yockey v. Salesforce, Inc*., 688 F. Supp. 3d 962, 969 (N.D. Cal. 2023). Yet that is precisely what the court purported to require in *BPS*. It held the plaintiff lacked standing based on his failure to satisfy the elements of a public disclosure of private facts claim or an intrusion upon seclusion claim. *BPS Direct*, 705 F.Supp.3d at 363-365. "In fact, in *TransUnion*, the Supreme Court found that the plaintiff's claim of harm can qualify for Article III standing, even if harm would not be established under the standards of the traditional harm the plaintiff's cause of action was closely related to." *Schnur v. JetBlue Airways Corp.*, 2024 WL 2816552, at *7 (W.D. Pa. June 3, 2024). "Violations of the right to privacy have long been actionable at common law," and "[a] right to privacy 'encompass[es] the individual's control of information concerning his or her persons.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598 (9th Cir. 2020) (citations omitted)). "[T]apping . . . telephone wires" is even an example of intrusion upon seclusion. Restatement (Second) of Torts § 652B cmt. b. (1977).

Besides, Plaintiffs' claim to standing is even stronger than it is for claims against defendants for sharing information with Facebook. Unlike cases involving Facebook, Plaintiffs have no relationship with AddShoppers. But because these retail defendants installed AddShoppers tracking code, AddShoppers received Plaintiffs detailed browsing activities on the retailers' websites. In other words, the retail defendants handed Plaintiffs' information to an unknown ad tracking company, not one with whom they had a preexisting relationship.

harms their privacy interest in any way."). In those cases, therefore, Plaintiffs generally lack any privacy interest unless they directly provided sensitive information to the website. *See Farst v. AutoZone, Inc.*, 7000 F.Supp.3d 222, 231 (M.D. Pa. 2023) ("Farst does not aver AutoZone disclosed . . . information that could potentially be used to identify him[.]").

At the hearing, Vivint downplayed the tracking scheme by likening it to a store clerk observing a customer shopping in a retail store. Tr. at *23, *26. But this analogy falls short; the AddShoppers tracking scheme is far more pernicious. A better analogy is AddShoppers supplies hidden cameras to retail stores, using facial recognition software to identify each shopper and link their in-store activities across multiple retailers without their knowledge or consent. Later, AddShoppers can send personalized letters encouraging shoppers to buy the items they viewed in store but didn't buy—taking a cut of every sale.[6] Compl. ¶ 42. This type of tracking—whether in person or on the internet—constitutes a privacy violation that consumers have the right to challenge in federal court.

C. Plaintiffs adequately allege a violation of the wiretapping statutes.

1. AddShoppers is not a party to Plaintiffs' communications with the retail defendants.

AddShoppers is not a party to Plaintiff Ingrao's communications with Nutrisystem. She did not intend to communicate with AddShoppers—she did not even know the ad tracking company existed. Instead, Plaintiff Ingrao only wanted to communicate with Nutrisystem's website. And Nutrisystem has no direct party defense where Plaintiff Ingrao "did not consent to

[6] Similarly, in this hypothetical world, session replay software is like a consulting firm hired to suggest improvements to the layout of the store. The consulting firm then employs someone to count the number of people who walk down the aisles and to observe the general paths they take through the store. The firm uses this anonymous information to recommend changes to the store's layout.

sending a separate message to [AddShoppers], was generally unaware of doing so, and had no control over that process." *Cole v. Quest Diagnostics, Inc.*, 2024 WL 3272789, at *4 (D.N.J. July 2, 2024). Nutrisystem's expansive view of the direct party exception to cover these circumstances would swallow the rule. *See id*. ("Adopting defendant['s] interpretation would undermine the protections intended by the statute by allowing entities to evade liability by structuring their technology to receive communications directly."). All embedded wiretap devices are designed to directly communicate with the third-party interloper. Thus, the inquiry must be whether the person intended to communicate with the third party who intercepted the communication. As the court in *Revitch* explained:

> [I]t cannot be that anyone who receives a direct signal escapes liability by becoming a party to the communication. Someone who presses up against a door to listen to a conversation is no less an eavesdropper just because the sound waves from the next room reach his ears directly. That person remains a third party, even as a direct recipient of the speaker's communication.

Revitch v. New Moosejaw, LLC, 2019 WL 545330, at *2 (N.D. Cal. Oct. 23, 2019).

Nor is Nutrisystem's expansive view of direct party exception compelled by *Google Cookie Placement*. There, the defendant placed content in the ad space on the websites that plaintiffs visited. *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 130 (3d Cir. 2015). The plaintiffs' web browsers therefore needed to send data to the defendant as a necessary condition for using the website. *Id*. at 142-43; Tr. at *44 ("Google was advertising or had advertising on the retailer's website."). The plaintiffs alleged that, in the process of inserting these ads into the websites, the defendant secretly placed extra tracking code into the web browsers, allowing them to track the users' behavior and serve them targeted content on pages visited later. *Id*. at 130-31. In other words, plaintiffs intended to communicate with the defendant but argued they were deceived into sharing *more data* than they had intended. Under these

circumstances, the Third Circuit held that the defendant remained a party to the communication, despite having exceeded the scope of consent. *Id*. at 142-43.

By contrast, Plaintiff Ingrao was never aware she was communicating with AddShoppers, never consented to do so, and there is no suggestion that Nutrisystem needs to send information to AddShoppers for its website to function (it certainly does not). Unlike in *Google Cookie Placement*, where data was exchanged directly with the defendant, Plaintiff Ingrao alleges that her information was surreptitiously shared with AddShoppers *in addition* to Nutrisystem. Because Plaintiff Ingrao's view of the direct party exception is consistent with the Ninth Circuit and California district courts, Doc. 39 at 20-21 (collecting cases), the Court should be particularly hesitant to extend the direct party exception to new circumstances where the party did not intend to communicate with the third party at all. *See Unified Sch. Dist. v. Newdow*, 542 U.S. 1, 16 (2004) ("Our custom on questions of state law ordinarily is to defer to the interpretation of the Court of Appeals for the Circuit in which the State is located.").

2. AddShoppers collected the content of Plaintiffs' communications with the retail defendants.

AddShoppers' tracking code collected the content of Plaintiffs' communications with websites. Specifically, this code is designed to intercept a person's electronic conversation with a website including the precise webpages they visit ("detailed referrer Uniform Resource Locator").[7]

[7] Although Plaintiffs allegations about AddShoppers tracking code are sufficient at this stage, Plaintiffs have recently discovered this code collects other communication content like search queries and products viewed or added to carts. *See In re Vizio, Inc., Consumer Priv. Litig.*, 2017 WL 11420284, at *6 (C.D. Cal. July 25, 2017) ("'samples' of the actual content displayed on a consumer's screen" are message content because "[w]hen watching a program through a connected device or streaming service, the 'intended message conveyed by the communication' is the program that the consumer is watching") (citing *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014)); *In re Google RTB Consumer Priv. Litig.* , 606 F.Supp.3d 935, 949 (N.D. Cal. 2002) (content adequately alleged where plaintiff allege defendant collected details, among other things, about the publisher object of the site and details about the contents within the site.).

Compl. ¶ 37. Although *McClung* is the only court to consider whether this specific code collects the content of a communication (concluding it does), *McClung*, 2024 WL189006, at *3, many courts have considered whether Facebook's substantially similar code collects the content of a communication and they have all reached the same conclusion, finding it intercepts detailed user interactions with websites. *See Cole v. Quest Diagnostics, Inc.*, 2024 WL 3272789, at *4 (D.N.J. July 2, 2024); *Braun*, 2023 WL 7544160, at *4 (collecting cases); *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 795–96 (N.D. Cal. 2022).

3. Plaintiffs did not consent to being tracked.

Vivint argues that Plaintiff Pacana consented to the terms and conditions by visiting the website.[8] Tr. at *57. But these terms and conditions were found in a browsewrap agreement. And "[b]rowsewrap agreements are properly viewed with skepticism because they purport to create binding contracts on terms a user is not required to review, and in the absence of any affirmative manifestation of agreement by the user." *Motley v. ContextLogic, Inc.*, 2018 WL 5906079, at *2 (N.D. Cal. Nov. 9, 2018). "[W]hether the terms and conditions in browsewrap agreements are enforceable, often turn[s] on whether the terms or a hyperlink to the terms are reasonably conspicuous on the webpage[]' such that a reasonably prudent user would have actual or constructive notice of the relevant conditions." *Oliver* v. Noom, 2023 WL 8600576, at *9 (W.D. Pa. Aug. 22, 2023). These terms were not reasonably conspicuous. As Vivint acknowledged, "there is no box that pops up. There's no consent to terms and conditions. That is merely available if you

[8] Vivint has suggested Plaintiffs consented because many websites deploy tracking software. But "the commonplaceness of any device or object is not the criterion for determining the innocence or criminality of its employment." *Commonwealth v. Murray*, 223 A.2d 102, 108-09 (Pa. 1966). And this argument is particularly weak under these circumstances. AddShoppers' tracking code is unique from other software on most websites for two reasons. First, it associates personal information with detailed browsing history. Second, consumers have no relationship with AddShoppers unlike Facebook or Google.

click on the hyperlink to take you to the terms and conditions." Tr. at *60. Accordingly, Vivint cannot show constructive or actual notice based on terms and conditions buried at the end of the webpage. Doc. 39 at 22-23. In any event, Vivint does not challenge the timing of the wiretap, which began before Plaintiff Pacana could even ostensibly consent. Doc. 39 at 22. So no matter how Vivint presented its terms and conditions, Plaintiff Pacana was wiretapped before she could even conceivably consent. *Id*.

4. Plaintiff Ingrao adequately pleads her communications were intercepted in Pennsylvania.

Nutrisystem incorrectly argues the sole interception point is where Plaintiff Ingrao's browser is located. Tr. at *65-66. But the Third Circuit stated in *Popa* that an interception could not also "occur where the information is ultimately received by the 'listener.'" *Popa v. Harriet Carter Gifts, Inc.*, 54 F.4th 121, 131 n.7 (3d Cir. 2022) (summary judgment). At this stage, it would be premature to determine where the interception occurred until the Parties had the benefit of discovery. Thus, the Court should wait for a fully developed record before deciding where Plaintiff Ingrao's communications were intercepted.

CONCLUSION

For the above reasons, and those provided in the consolidated opposition to the motion to dismiss, Plaintiffs request that the Court deny Defendants' motions to dismiss in their entirety.

Dated: October 15, 2024

Respectfully submitted,

By: /s/ *Charles E. Schaffer*
Charles E. Schaffer
Nicholas J. Elia
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
cschaffer@lfsblaw.com

nelia@lfsblaw.com

Norman E. Siegel (*pro hac vice*)
J. Austin Moore (*pro hac vice*)
Kasey Youngentob (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100 (tel.)
siegel@stuevesiegel.com
moore@stuevesiegel.com
youngentob@stuevesiegel.com

Attorneys for Plaintiffs and the Class